REMARKS

This communication is a full and timely response to the non-final Office Action dated July 15, 2004 (Paper No. 14). By this communication, claim 3 has been canceled without prejudice, claims 8 and 14 have been amended, and claims 19 and 20 have been added.

Claim 8 was amended to correct antecedent matter and claim 14 was amended to change "when a fingerprint accepting flag is set in the second memory unit." Support for the changes to claim 14 can be found variously throughout the specification, for example, at page 7, lines 10-14 of the specification. No new matter has been added.

Claims 19 and 20 have been added. Support for the subject matter recited in claims 19 and 20 can be found variously throughout the specification and claims, for example, at page 7, lines 15-25, page 8, lines 1-11, and page 9, lines 19-23 of the specification. No new matter has been added.

Claims 1, 2, and 4-20 are pending where claims 1, 4, 5, 10, and 19 are independent.

Rejection Under §112, Second Paragraph

Claim 8 was rejected under 35 U.S.C. §112, second paragraph as indefinite. Applicant has addressed this matter by amending claim 8 to change "the personal computer" to "a personal computer." Accordingly, Applicant respectfully requests that the rejection of claim 8 under 35 U.S.C. §112, second paragraph should be withdrawn.

Rejections Under 35 U.S.C. §103

Claims 1-4 were rejected under 35 U.S.C. §103(a) as unpatentable over *Osten et al.*, U.S. Patent No., 5,719,950 in view of *Senior*, U.S. Patent No. 6,400,836. Applicant respectfully traverses this rejection.

Independent claim 1 recites a fingerprint collating device for collating a user's fingerprint with registered fingerprint information to effect personal authentication, said device comprising an external computer; a prism for reading said fingerprint to create read fingerprint information, and to create read history information indicating that said read fingerprint information has been created; a read history storage for storing said read history information and executing a control program when instructed by the external computer; a controller for setting a fingerprint accepting

flag associated with said read fingerprint information indicating that read fingerprint information is normally produced through said prism; and a collator collating said read fingerprint information with said registered fingerprint information to effect personal authentication and output a result of authentication when said fingerprint accepting flag is set, said read history information is stored in said read history storage, and the control program is executed.

Independent claim 4 recites a fingerprint collating method for collating a user's fingerprint with registered fingerprint information to effect personal authentication, said method comprising the steps of reading said fingerprint through a prism to create read fingerprint information, and to create read history information indicating that said read fingerprint information has been created; storing said read history information in read history storing means; setting a fingerprint accepting flag associated with said read fingerprint information indicating that read fingerprint information is normally produced through the prism; and executing a control program in said read history storage means when an instruction signal is received from an external computer; and collating said read fingerprint information with said registered fingerprint information to effect personal authentication and output a result of authentication when said fingerprint accepting flag is set, said read history information is stored in said read history storing means, and said read history storage means executes the control program.

In summary, when read fingerprint information is generated, the collating device determines whether the read fingerprint information was produced via a finger scan performed by a prism. If the read fingerprint information is determined to be the product of a finger scanned by the prism, the collation controller sets a fingerprint accepting flag. Once the fingerprint accepting flag is set collation between a fingerprint template and the read fingerprint information can be executed.

Osten discloses a biometric authentication system having fingerprint sensor 10 and non-specific biometric sensors 24, 26, and 28. The fingerprint sensor 10 captures the image of a fingerprint. Then an image processor 12 converts the image into a vector array of the fingerprint minutiae. A comparator 14 correlates the vector array of the captured image with an array that is associated with a PIN and acquired from a memory file 16. The pre-stored fingerprint pattern is stored in either a dedicated ROM memory of the system, in the memory of the computer terminal accessed by the individual, or entered via a magnetic card. The Office Action acknowledges that

Osten fails to disclose, teach, or suggest setting a fingerprint accepting flag associated with said read fingerprint information indicating that read fingerprint information is produced through said prism. The Office Action then relies on *Senior* to remedy this deficiency.

Senior discloses a fingerprint authentication system that captures a fingerprint image via a scanner 130 (step 420, 430). The acquired image is compared with stored fingerprint characteristics (440). When the acquired fingerprint is recognized as a match a status or authentication flag is set (470). The status flag and the matching fingerprint coordinates are transmitted to a computer 100 (490). The authentication flag may be set for an indefinite period or a predetermined period, but is contingent on whether a fingerprint match is detected. Namely, if ever a high quality fingerprint is obtained that does not match an authorized user, the authentication flag is unset, and the operation of the computer 100 suspended. Based on at least these teachings it is apparent that *Senior* fails to disclose, teach, or suggest setting a fingerprint accepting flag associated with said read fingerprint information indicating that read fingerprint information is normally produced through said prism. *Senior* discloses that the authentication flag is set when a good quality, verifiable print is presented by the user and then verified by the recognition system. Fig. 4 further supports this teaching, where it shows that the authentication status flag (470) receives its input not from the fingerprint image acquisition block (420), but the fingerprint recognition system (440). In other words, the authentication flag is set when an acquired fingerprint is verified or recognized by the system as a fingerprint of an authorized user. For at least these reasons, *Senior* does not remedy the deficiencies of *Osten*.

In sum, *Osten* and *Senior* either singly or combined fail to disclose, teach, or suggest at least setting a fingerprint accepting flag associated with said read fingerprint information indicating that read fingerprint information is produced through said prism. At best, the references combine to teach that an authentication flag is set when an acquired fingerprint is verified or recognized by the system as a fingerprint of an authorized user. In other words, the authentication flag is set after collation is performed, or when the acquired fingerprint information is compared against fingerprint information stored in a database. Accordingly, this flag is not analogous to the flag recited in claims 1 and 4. Thus, a *prima facie* case for obviousness has not been established.

To establish *prima facie* obviousness of a claimed invention, all of the claim limitations

must be taught or suggested by the prior art. In re Royka, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). Moreover, obviousness "cannot be established by combining the teachings of the prior art to produce the claimed invention, absent some teaching or suggestion supporting the combination." ACS Hosp. Sys. V. Montefiore Hosp., 732 F.2d 1572, 1577, 221 USPQ 929, 933 (Fed. Cir. 1984). Accordingly, Applicant respectfully requests that the rejection of claims 1 and 4 under 35 U.S.C. §103 be withdrawn, and these claims be allowed.

Claims 2 and 3 depend from claim 1. By virtue of this dependency, Applicant submits that claims 2 and 3 are allowable for at least the same reasons given above with respect to claim 1. In addition, Applicant submits that claims 2 and 3 are further distinguished over *Osten* and *Wang* by the additional elements recited therein, and particularly with respect to each claimed combination. Applicant respectfully requests, therefore, that the rejection of claims 2 and 3 under 35 U.S.C. §103 be withdrawn, and these claims be allowed.

Claims 5-18 were rejected under 35 U.S.C. §103(a) as unpatentable over *Oster* in view of *Senior* in view of *Johnson*, U.S. Patent No. 3,619,060. Applicant respectfully traverses this rejection.

Claim 5 recites a fingerprint collating system comprising means for generating a collation instruction and an index number; means for illuminating a bottom face of a prism based on the collation instruction; means for generating a fingerprint image of a user when an air layer exists between a finger of a user and a top face of the prism; means for setting a fingerprint accepting flag in a first memory unit when a fingerprint image of the user is normally produced through the prism; means for reading a fingerprint template associated with the index number from a second memory unit; and means for collating the fingerprint image and the fingerprint template when the fingerprint image of the user is generated and the fingerprint accepting flag is set.

Claim 10 recites a method for collating a fingerprint in a fingerprint collating system that includes a personal computer and a collating unit, the method comprising generating a collation instruction and an index number; illuminating a bottom face of a prism based on the collation instruction; generating a fingerprint image of a user when an air layer exists between a finger of a user and a top face of the prism; setting a fingerprint accepting flag in a first memory unit when a fingerprint image is normally produced through the prism; reading a fingerprint template associated with the index number from a second memory unit; and collating the fingerprint

image and the fingerprint template when the fingerprint image of the user is generated and the fingerprint accepting flag is set.

In summary, when read fingerprint information is generated, the collating device determines whether the read fingerprint information was produced via a finger scan performed by a prism. If the read fingerprint information is determined to be the product of a finger scanned by the prism, the collation controller sets a fingerprint accepting flag. Once the fingerprint accepting flag is set collation between a fingerprint template and the read fingerprint information can be executed.

The Office Action acknowledged that *Osten* does not explicitly disclose means for illuminating a bottom face of a prism based on the collation instruction, and relied on *Johnson* to remedy this deficiency nor does *Osten* disclose setting a fingerprint accepting flag in a first memory unit when a fingerprint image is normally produced through the prism.

As discussed above, *Senior* also fails to disclose, teach, or suggest at least setting a fingerprint accepting flag in a first memory unit when a fingerprint image is normally produced through the prism, and thus fails to remedy the deficiencies of *Osten*.

Johnson discloses an identification device having a prism 18. The prism is provided with a first face 20, a second face 22 disposed at an angle to the first face, and a third face 24 disposed at an angle to the second face 22. When identifying a fingerprint, the user places a finger on the second face 22. A light beam 16 that is perpendicular to the first face 20 then passes through the prism 18 and an image is formed. The image is generated through the glass-air interface formed on the second face 22 where the light beam 16 will not be reflected at those points where something touches the interface and thus destroys the index of refraction ratio of the glass and the air. *Johnson*, however, fails to disclose, teach, or suggest at least setting a fingerprint accepting flag in a first memory unit when a fingerprint image is normally produced through the prism. In fact, *Johnson* is not capable of setting or storing an accepting flag because it is comprised of analog elements.

In sum, *Osten*, *Senior*, and *Johnson* either singly or combined fail to disclose, teach, or suggest at least setting a fingerprint accepting flag in a first memory unit when a fingerprint image is produced through the prism. At best, the references combine to teach that an authentication flag is set when an acquired fingerprint is verified or recognized by the system as

a fingerprint of an authorized user. In other words, the authentication flag is set after collation is performed, or when the acquired fingerprint information is compared against fingerprint information stored in a database. Accordingly, this flag is not analogous to the flag recited in claims 5 and 10. Thus, a *prima facie* case for obviousness has not been established.

To establish *prima facie* obviousness of a claimed invention, all of the claim limitations must be taught or suggested by the prior art. In re Royka, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). Moreover, obviousness "cannot be established by combining the teachings of the prior art to produce the claimed invention, absent some teaching or suggestion supporting the combination." ACS Hosp. Sys. V. Montefiore Hosp., 732 F.2d 1572, 1577, 221 USPQ 929, 933 (Fed. Cir. 1984). Accordingly, Applicant respectfully requests that the rejection of claims 5 and 10 under 35 U.S.C. §103 be withdrawn, and these claims be allowed.

Claim 14 recites a system for collating a fingerprint of a user, comprising a computer that generates a fingerprint collation instruction and an index number, wherein the computer has a first memory unit; a prism that generates a fingerprint image of a user when the collation instruction is received from the computer and an air layer exists between a portion a finger of the user and a top face of the prism; and a collating unit that retrieves a fingerprint template of the user from a second memory unit based on the index number and collates the fingerprint image of the user with the fingerprint template when a fingerprint accepting flag is set in the first memory unit, wherein the fingerprint accepting flag is set when a fingerprint image is normally produced through the prism.

In summary, when read fingerprint information is generated, the collating device determines whether the read fingerprint information was produced via a finger scan performed by a prism. If the read fingerprint information is determined to be the product of a finger scanned by the prism, the collation controller sets a fingerprint accepting flag. Once the fingerprint accepting flag is set collation between a fingerprint template and the read fingerprint information can be executed.

As discussed above, *Osten*, *Senior*, and *Johnson* either singly or combined fail to disclose, teach, or suggest at least setting a fingerprint accepting flag in a first memory unit when a fingerprint image is produced through the prism. At best, the references combine to teach that an authentication flag is set when an acquired fingerprint is verified or recognized by the system

as a fingerprint of an authorized user. . In other words, the authentication flag is set after collation is performed, or when the acquired fingerprint information is compared against fingerprint information stored in a database. Accordingly, this flag is not analogous to the flag recited in claim 14. Thus, a *prima facie* case for obviousness has not been established.

To establish *prima facie* obviousness of a claimed invention, all of the claim limitations must be taught or suggested by the prior art. In re Royka, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). Moreover, obviousness "cannot be established by combining the teachings of the prior art to produce the claimed invention, absent some teaching or suggestion supporting the combination." ACS Hosp. Sys. V. Montefiore Hosp., 732 F.2d 1572, 1577, 221 USPQ 929, 933 (Fed. Cir. 1984). Accordingly, Applicant respectfully requests that the rejection of claim 14 under 35 U.S.C. §103 be withdrawn, and this claim be allowed.

Claims 6-9 depend from claim 5, claims 11-13 depend from claim 10, and claims 15-18 depend from claim 14. By virtue of this dependency, Applicant submits that claims 6-9, 11-13, and 15-18 are allowable for at least the same reasons given above with respect to claims 5, 10, and 14, where applicable. In addition, Applicant submits that claims 6-9, 11-13, and 15-18 are further distinguished over *Osten*, *Senior*, and *Johnson* by the additional elements recited therein, and particularly with respect to each claimed combination. Applicant respectfully requests, therefore, that the rejection of claims 6-9, 11-13, and 15-18 under 35 U.S.C. §103 be withdrawn, and these claims be allowed.

Newly Added Claims

Claim 19 recites a fingerprint collating device for collating a user's fingerprint with registered fingerprint information to effect personal authentication, said device comprising an external computer; a prism for reading said fingerprint to create read fingerprint information, and to create a fingerprint accepting flag indicating that said read fingerprint information has been created; a first memory unit for storing said fingerprint accepting flag and executing a control program when receiving a collating instruction and an index number of the user from said external computer; a second memory unit for registering a plurality of fingerprint templates corresponding to each received index number of said registered fingerprint information; a controller for setting a fingerprint accepting flag associated with said read fingerprint

information indicating that read fingerprint information is normally produced through said prism; and a collator for collating said read fingerprint information with one of said plurality of fingerprint templates corresponding to said received index number to effect personal authentication when said fingerprint accepting flag is set, and outputting a result of the authentication to said external computer, wherein said fingerprint accepting flag is reset when said collating is complete.

In summary, when read fingerprint information is generated, the collating device determines whether the read fingerprint information was produced via a finger scan performed by a prism. If the read fingerprint information is determined to be the product of a finger scanned by the prism, the collation controller sets a fingerprint accepting flag. Once the fingerprint accepting flag is set collation between a fingerprint template and the read fingerprint information can be executed.

Osten, *Senior*, and *Johnson* either singly or combined fail to disclose, teach, or suggest at least one of said fingerprint template corresponding to said received index number to effect personal authentication when said fingerprint accepting flag is set, setting a fingerprint accepting flag associated with said read fingerprint information indicating that read fingerprint information is produced through said prism, and outputting result of authentication to said external computer. For at least this reason, Applicant respectfully requests that claim 19 be considered and allowed.

Claim 20 depends from claim 19. By virtue of this dependency, Applicant submits that claim 20 is allowable for at least the same reasons discussed above. Accordingly, Applicant respectfully requests that claim 20 be considered and allowed.

Conclusion

Based on at least the foregoing amendments and remarks, Applicant submits that claims 1, 2, and 4-20 are allowable, and this application is in condition for allowance. Accordingly, Applicant requests favorable reexamination and reconsideration of the application. In the event the Examiner has any comments or suggestions for placing the application in even better form, Applicant requests that the Examiner contact the undersigned attorney at the number listed below.

Applicant believes no fee is due with this response. However, if a fee is due, please charge our Deposit Account No. 18-0013, under Order No. SON-1889 from which the undersigned is authorized to draw.

Dated: October 1, 2004

Respectfully submitted,

By_____
Ronald P. Kananen
Registration No.: 24,104
Attorney for Applicant

RADER, FISHMAN & GRAUER, PLLC
Lion Building
1233 20th Street, N.W., Suite 501
Washington, D.C. 20036
Tel: (202) 955-3750
Fax: (202) 955-3751
Customer No. 23353